Notice of Allowability	Application No.	Applicant(s)	
	10/707,481	BURDINE ET AL.	
	Examiner	Art Unit	
	Chat C. Do	2193	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *07/12/2007 and attached interview dated 08/01/07*.

2. ☒ The allowed claim(s) is/are *1, 3-4, 6, and 8-12, as now re-numbered as 1-9*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *attached herein* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Kerry Goodwin, Reg. No. 48,955 on 08/01/2007.

The application has been amended as follows:

4. (Currently amended) A computer program product comprising a computer storage ~~useable~~ medium storing ~~having~~ a computer readable program, wherein the computer readable program when executed on a computer causes the computer to perform method steps for determining the Nth state of an n-stage linear feedback shift register (LFSR), providing a result useful in applications including password generation, convergent signature analysis, and encryption, said method comprising:

building a look-up table of n-bit states for latch positions of said linear feedback shift register;

obtaining a modulo remainder of said Nth state; and

generating directly from said modulo remainder and said n-bit states said Nth state and, if in standard form, further comprising steps of:

converting said LFSR to modular form;

modulo (2^n - 1) dividing a desired cycle count N to derive a remainder value N";

building said look-up table to include x, y, and z values, where

x=LFSR latch position (0, 1,..., n-l);

$y=2^i$ for i=0, n-1 (for i=0, 1, 2, 3,..., n-l), giving values (0, 1, 2, 4, 8,...,2^{n-1}); and

z=n-bit state of said LFSR for (x, y);

identifying for each bit set in said remainder value N" a corresponding cycle row y;

for a first identified cycle row in N", determining from said look-up table a corresponding n-bit state $S_{first\_cycle\_row}$;

for each bit set in said n-bit state $S_{first\_cycle\_row}$, next determining from said look-up table a next corresponding n-bit state $S_{first\_cycle\_row}$;

repeating said next determining step until all final states $S_{first\_cycle\_row}$ are reached for said bit set in said n-bit state $S_{first\_cycle\_row}$;

exclusive ORing all said final states for said bit set in said n-bit state;

repeating said determining steps until processing all bits set in said LFSR; and

exclusive ORing all said final states for all said bits set in said LFSR to determine said Nth state of said LFSR.

2. Claims 1, 3-4, 6, and 8-12 are allowed.

3. Claims 2, 5, and 7 are cancelled.

4. The following is an examiner's statement of reasons for allowance:

The prior art of records fail to disclose or render an obviousness of a method, medium, and system for determining the N^{th} stage of an n-stage LFSR that would be useful in many practical applications comprising: building a look-up table for LFSR; obtaining a modulo remainder of the Nth stage; and further comprising steps if in standard form, converting said LFSR to modular form; modulo $(2^n - 1)$ dividing a desired cycle count N to derive a remainder value N"; building said look-up table to include x, y, and z values, where x=LFSR latch position (0, 1,..., n-l); $y=2^i$ for i=0, n-1 (for i=0, 1, 2, 3,..., n-l), giving values (0, 1, 2, 4, 8,...,2^{n-1}); and z=n-bit state of said LFSR for (x, y); identifying for each bit set in said remainder value N" a corresponding cycle row y; for a first identified cycle row in N", determining from said look-up table a corresponding n-bit state $S_{first\_cycle\_row}$; for each bit set in said n-bit state $S_{first\_cycle\_row}$, next determining from said look-up table a next corresponding n-bit state $S_{first\_cycle\_row}$; repeating said next determining step until all final states $S_{first\_cycle\_row}$ are reached for said bit set in said n-bit state $S_{first\_cycle\_row}$; exclusive ORing all said final states for said bit set in said n-bit state;repeating said determining steps until processing all bits set in said LFSR; and exclusive ORing all said final states for all said bits

set in said LFSR to determine said Nth state of said LFSR along with other features as cited in the independent claims 1, 4, and 6.

The closest found prior art is Ward et al. (U.S. 4,142,240). Ward et al. disclose a method for determining a N^{th} state of n-stage LFSR comprising steps of building a look-up table and obtaining a modulo remainder of the N^{th} state. However, Ward et al. fail to disclose the steps in standard form comprising converting said LFSR to modular form; modulo $(2^n - 1)$ dividing a desired cycle count N to derive a remainder value N"; building said look-up table to include x, y, and z values, where x=LFSR latch position (0, 1,..., n-l); $y=2^i$ for i=0, n-1 (for i=0, 1, 2, 3,..., n-l), giving values (0, 1, 2, 4, 8,...,2^{n-1}); and z=n-bit state of said LFSR for (x, y); identifying for each bit set in said remainder value N" a corresponding cycle row y; for a first identified cycle row in N", determining from said look-up table a corresponding n-bit state $S_{first\_cycle\_row}$; for each bit set in said n-bit state $S_{first\_cycle\_row}$, next determining from said look-up table a next corresponding n-bit state $S_{first\_cycle\_row}$; repeating said next determining step until all final states $S_{first\_cycle\_row}$ are reached for said bit set in said n-bit state $S_{first\_cycle\_row}$; exclusive ORing all said final states for said bit set in said n-bit state;repeating said determining steps until processing all bits set in said LFSR; and exclusive ORing all said final states for all said bits set in said LFSR to determine said Nth state of said LFSR as seen above.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue

fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chat C. Do whose telephone number is (571) 272-3721. The examiner can normally be reached on Tue-Fri 9:00AM to 7:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (571) 272-3756. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Chat C. Do
Examiner
Art Unit 2193

August 2, 2007